IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 45-49
www.iosrjournals.org

Applying Cipher Technique Using Key-Aggregate Searchable Method For Multi Data Sharing Via Cloud Storage

Pawar .S.S. [1], Rayate .M.H.[2] Ghuge.P.R[3], Sonawane .A. S[4,] A. A. Pundlik[5]
1, 2, 3, 4, 5(Dept of Comp. Engg., KVNNIEER, S.P.P.U., MS, India)

Abstract: *In cloud storage data sharing is the most valuable activity to perform necessary actions. In this article, we show how to share data with others in cloud database in an efficient, reliable, secure and scalable manner. We explain new public-key cryptography for efficient allocation of decryption rights for any set of cipher texts is possible that generate static-size encryption. The innovation is that one can collectively gather any set of secret keys makes them as compact as a single key, but surrounding the power of all the keys being collective at surrounding. In other aspects, the secret key user can release a constant-size collective key for selection purpose of cipher text set in cloud database, but the other encrypted files outside the set remain confidential. This compact collective key can be stored in a smart card or efficiently sent to others with very limited secure database. In the standard model, we offer formal security investigation of our schemes. We also evaluate other application of our schemes. In particular, our framework gives the first public-key patient-controlled encryption for scalable hierarchy, which was yet to be known.*

Keywords : *Aggregate key, Encryption, Searching, Security, Sharing.*

I. Introduction

This new trend is called cloud computing and, not pressingly it's linked to interprets inexorable rise. What is cloud computing? How does it work? Let's take a closer look! Recently Cloud storage has emerged as a prominent solution for resourcing present, convenient and required accesses to huge amounts of data shared over the social media all over the world.

Now a day's millions of users are sharing their personal data, including texts, images, audios and videos, with another users through social networking applications which is totally based on cloud storage technology. Because of the beneficial applications of the cloud storage such as cheap cost, easy accessing, huge storage capacity many professionals and businessman's are being attracted towards cloud storage technology. It is also getting more attention due to its expandability feature.

Now a day's data redistribution is also clamorous day by day so the most critical problem being faced by the users is about security issues of the personal data and communication among business intelligence of specific firmware i.e. recent case of online leakage of bank details of a business personal.[1]To overcome such kind of problem user can use cipher technique by converting users original data which is present in readable text to encrypted format that means unreadable text, so the data will be get protected from the unauthorized access by the hackers and intruders. Simultaneously the same data can be get retrieved from the cloud by performing decryption process on the data which is already present in encrypted that means cipher text format over the cloud.

Cloud system is most rousted entity hence data directly stored on cloud is not surely secure. Also cloud is safe but investigation hence senile information has to be protected with the help of cipher technique. Sharing of such cipher data is grievance on cloud services because every time new encryption keys are generated and this key management becomes miscellaneous task. Pay-as-you-use is the rule of cloud as far as cost-effective view is concern. Hence for key management additional avoidable usage of cloud arise which makes system more excessive Hence there must be system which works on efficient management of these encryption keys, adequate data sharing, encryption of data over cloud. By analyzing all the techniques as well as their issues related to data sharing over cloud system. We propose a system called as "KASE". This system can address the problem with existing system, such as, Public Key Encryption with keyword Search approach. Many existed systems offered from threats such as, those systems are systems are impractical and disorganized as they may require many keys over the cloud data for encryption as well as decryption. Our goal is to analyzed users issues related to their database and define general platform for KASE system, to provide strong data security, Easy Data sharing, closeness Search strength and appointment.

II. Related Work

Cloud computing is important concept of computing in which resources of the computing base structure are on condition that as service over the internet.[2] As making statement of undertaking as it is, this example also takes forth many new question for facts safety and way in control when users get work done by others sensitive knowledge for computers for having the same on cloud server, which are not within the same law domain as facts owners. The hard question of at the same time fine-grainedness, scalability and knowledge for computers secretly of way in control actually still remains unresolved. This paper focuses this hard open question under discussion by, on one hand, making clear and putting into operation way in policies based on facts properties.

safe provenance that stores being owner and process history of data ends is full of force to the good outcome of data forensics in cloud computing, yet it is still a hard issue under discussion today.[3] In this paper, to apparatus this unseen area in cloud computing technique, we made an offered a new secure provenance design based on the bilinear putting together expert way of art and so on. As the essential bread and butter of data forensics and post observations in cloud computing, the made an offered design is represented by providing the information secretly on sensitive forms stored in cloud, name not given authentication on users way in, and provenance going after by signs on questioned printed materials.

It is desirable to stores facts on knowledge for computers place for storing computers such as post computers and text record computer in encrypted form to get changed to other form safety and right not to be public dangers.[4] But this usually suggest that one has to offering workings for safety. In this paper, we make, be moving in our cryptographic designs for the hard point of looking for on encrypted facts and provide facts in support of safety for the coming out crypto system. Our techniques have a number of important better chances. They are provably safe: they give provable secrecy for encryption, in the case that the un-trusted computer cannot learn anything about the plain text when only given the cipher wording; they make ready queries away from other things for searches, that is that the un-trusted computer cannot studied anything more about the plain text than the look for outcome; they make ready controlled looking for, so that the un-trusted computers cannot look for a not based on rules word without the users authority; they also support put out of the way question, so that the user may question the un law computer to look for a secret word without letting be seen the word to the computer.

With cloud computing technique and place for storing help, facts is not only stored in the cloud, but in a regular order shared among a large number of users in a group.[6] In this paper, we make an offer Knox, a privacy preserving looking over of account by expert apparatus for facts stored in the cloud and shared among a greatly sized number of users in a group. In particular we put to uses group signatures to make homomorphic authenticators, so that a third group suprintendent (TPA) is able to make certain of the true, good nature of shared knowledge for computers for users without getting back the complete facts. With Knox, the amount of information used for verification, as well as the time it takes to looking over of account by expert with it, are not acted-on according to the rules of users in the group. In addition, Knox great acts homomorphic MAC to get changed to other form the space used to store such verification information our testing result play or amusement that Knox is able to with small amount of money looking over of account by expert the rightness of facts, shared among a large number of users. With cloud computing and place for storing, user are able to way in and to part resources offered by cloud public organization givers at a lower marginal price.

Cloud computing technique is a coming out of computing example. It provides a money-related and good at producing an effective answer for having the same group support among cloud users. Needing payment to frequent change of members in more than one or owner group, keeping safe user fact and their mind and physical qualities right not to be public becomes a hard offspring in cloud.[7] Several safety designs for knowledge for computers having the same on untrusted computers have been made an offered. In these moves near, facts owners store the encrypted knowledge for computers stores in untrusted place for storing and make distribution the being like decryption keys only to given authority users. In this way, not with authority user as well as place for storing computers cannot learn the what is in of the facts records because they have no knowledge about decryption keys. However, the complex conditions of user taking-part and revocation in these design are linearly increasing with the number of facts owners and the number of put an end to users, separately. By frame for event a group with a single property, Lu et Al put forward a safe provenance design based on the cipher text attribute-based encryption way of doing, which lets any part in a group to part knowledge for computer with others. However, the question under discussion of user revocation is not made house number in their design. Yu et Al presented scalable and fine-grained facts way in control design in cloud computing depends on the key insurance agreement attribute based encryption trained way of art and so on.

III. Proposed System

Aaccording to analysis of an existing system we solved the issues like uploading data using class concept also decrypting class with a single aggregate key.

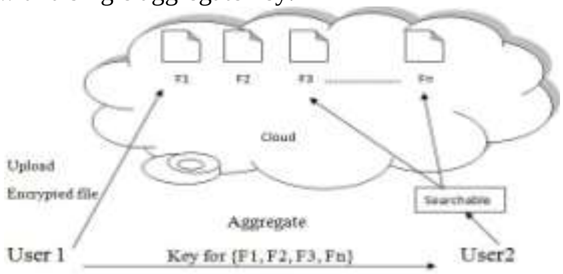

Fig. 1. Architecture of KASE system

In our system user can easily registered on cloud system and also can be easily encrypts the data along with master key as well as aggregate key due to which the original data of the user get converted into cipher text which is unable to understand for another users. While in an existing system there in no such concept of an aggregate key so we propose a new system i.e. KASE system in which by an aggregate key multiple amount of data can easily uploaded and get decrypted. Here another user can only decrypt the data while can't modify the data. For this data user have a unique key i.e. master key with the help of this key user can easily upload and download data in the form of encryption and decryption also for same data user generate unique key i.e. an aggregate key for particular user who can easily decrypts the data with the help of aggregate key and receives original data uploaded by data owner.

While uploading data on the cloud we can easily add multiple files to the class by providing a master key which is already generated at the time of user registration which is provided by the system for specific user name or we can also create a new class except the system classes and process for the same task i.e. adding files into the class after adding files to the class we process for the next that is upload the files on the system. After uploading files on the cloud, system get generates some specific keywords for particular file which is get uploaded on the cloud for which we can easily search a particular file among multiple files present on the cloud system. The file which we want search on the cloud then keywords of the files get stored at index location through which we uses the keywords belong to that file and in this way we can easily receive particular file as we want .

IV. Algorithm

4.1 Algorithm for Aggregate Key Generation Process:

Input: key1: Master-Key,
key2: Class Key,
key3: Code.

Output: Aggregate key.

Process:

1. First Setup Data.
2. All the keys like k1, k2, k3 are in string format then it will converted into bytes using
Byte Encoder.
3. Then every string converted in string to number like,
k1=123
k2=564
k3=356
4. All set key combine then it can give separator for that different key like 123 0 5640.356 here no value consider as separator.
5. Secrete key i.e, S.
6. Key convolution: we are use the quadratic equation,
$F(x) = (n1x + n2\ x2 + S)$
Here the x is considered as 2 or any number.
7. Display key.

4.2 Algorithm for AES Algorithm:

Input: secret key k, Message M

Output: Encrypted Message EM

Process:

1. Key Expansions round: keys are derived from the cipher key using Rijndael's key schedule. AES needs a separate 128-bit round key block for each round plus one more.
2. Starting Round: Add Round Key each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds:

•Sub Bytes a non-linear substitution step where each byte is replaced with another according to a lookup table.
•Shift Rows a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
•Mix Columns a mixing operation which operates on the columns of the state, combining the four bytes in each column.
•Add Round Key

4. Finishing Round (no Mix Columns)

•S Sub Bytes.
•Shift Rows.
•Add Round Key.

V. Mathematical Model

Let S be the KASE framework,
S = {I, O, P }
Where,
I = {Master key, Documents}
O = {Keywords }
P = {f1, f2, f3, f4, f5, f6, f7 }
Where,
f1 = {Setup (1^{λ}, n) : the cloud server initialize system parameters. }
$g_i = g^{(\alpha i)} \in G$
For i = {1, 2, ……. n, n + 2, …….., 2n }
f2 = {Keygen (pk, msk) : data owner to generate key pair. }
$pk = v = g^{\gamma}; msk = \gamma$
f3 = {Encrypt (pk, i): to encrypt data and generate its keyword cipher texts when uploading the i-th document. }
$c_1 = g^t, c_2 = (v.g_i)^t$
$c_w = e(g, H(w))^t / e(g1, g_n)^t$
f4 = { Extract(msk, S): to generate an aggregate searchable encryption key. }
Subset S € { 1, ……….., n }
$k_{agg} = \pi_{j \in s\, g^{\gamma} n+1-j*}$
f5 = { Trapdoor (k_{agg}, w) : to generate the trapdoor to perform keyword search. }
$TR = k_{agg}.H(w)$
f6 = {Adjust(params, i, S, Tr): the cloud server produce the right trapdoor. }
index i ϵ S
$Tr_i = Tr, \pi_{j \in s, j \neq i g n+1-j+i}$
f7 = {Test (Tr_i, i): to perform keyword search over the i-th document. }
$c_w = = e(Tr_i, c_1) / e(pub, c_2)$
$pub = \pi_{j \in s g n+1-j}$

VI. Experimental Setup

To implement our system we have to need following platform on both side i.e. client and server. At client side we use operating systems like Linux, windows. We also uses web browsers such as Chrome, Mozilla Firefox etc. For database as well as network connection we uses modem drivers. For processing the data in the form of user and system communication we uses JRE1.7 and at server side we uses the same configuration including apache tomcat 7.0.56 while at developer side we uses some tools that is Dreamweaver 8 / Adobe CS3For HTML ,CSS , JavaScript , AJAX , XML editing ,Browsers (Latest Versions)Chrome, Mozilla Firefox etc. to test servlet WAMP / XAMPP 3.2.1 (And above)Eclipse–Helios (or Above Versions)For JAVA code editing and for hardware platform we use processor Min core- i3, RAM Min 2 GB and Hard Disk40GB.

VII. Conclusion

In the KASE system the user receive only one aggregate key for encryption and decryption of the data on public cloud database. The KASE system also condensed the use of number of trapdoors under multi owner system. By using the KASE system the reduction of generates the multiple keys for the various documents or files. Both analysis and evaluation result confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage.

VIII. Future Scope

First time introduced such kind of technique to minimize multiple keys and overcome data redundancy over multiple users by generating a single key. With the help of this approach user can provide effective solution to building real time data sharing system based on public cloud database. It is also used in future to work for provide the solution for KASE in the case of linked cloud.

References

[1] Baojiang Cui, Zheli Liu and Lingyu Wang, “Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage ", Proc. IEEE Press, pp.year 2015.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, " Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing ", Proc. IEEE INFOCOM, pp. 534-542, 2010.

[3] R. Lu, X. Lin, X. Liang, and X. Shen, " Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing ", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[4] X. Song, D.Wagner, A. Perrig. “Practical techniques for searches on encrypted data ", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

[5] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "` Public Key Encryption with Keyword Search ", EUROCRYPT 2004, pp. 506C522, 2004.

[6] C. Chu, S. Chow,W. Tzeng, et al. " Key-Aggregate Crypto system for Scalable Data Sharing in Cloud Storage ", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[7] X. Liu, Y. Zhang, B. Wang, and J. Yan. “Mona: secure multi owner data sharing for dynamic groups in the cloud ", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.

[8] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. “Searchable symmetric encryption: improved definitions and efficient constructions ", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[9] P. Van,S. Sedghi, JM. Doumen. " Computationally efficient searchable symmetric encryption ", Secure Data Management, pp. 87-100, 2010.

[10] S. Kamara, C. Papamanthou, T. Roeder. “Dynamic searchable symmetric encryption ", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965-976, 2012.

[11] Y. Hwang, P. Lee. “Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System ", In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.Commun. Secur., 2013, pp. 1029–1042.